Spis treści

[Macierz dyskowa 2 szt. 1](#_Toc202190703)

[Serwer bazodanowy 2 szt. 1](#_Toc202190704)

[Serwer wirtualizacyjny 3 szt. 1](#_Toc202190705)

[Rozbudowa switch FC 2 szt. 1](#_Toc202190706)

[Baza danych 2 szt. 1](#_Toc202190707)

[Wirtualizacja 2](#_Toc202190708)

[System operacyjny 2](#_Toc202190709)

[Okablowanie 2](#_Toc202190710)

# Macierz dyskowa 2 szt.

Ogólne

● System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 2U w tej szafie. Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). Każdy moduł/obudowa powinien posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii.

● Macierz musi umożliwiać takie podłączenie półek aby awaria lub/i usunięcie jednej z półek nie powodowało utraty dostępu do danych znajdujących się na pozostałych modułach.

● Macierz musi obsługiwać min. 440 dysków wykonanych w technologii hot-plug.

● Macierz musi obsługiwać min. 120 dysków wykonanych w technologii SSD.

● Macierz musi posiadać 4 porty SAS 12 Gb/s do podłączenia dodatkowych półek dyskowych.

Pojemność macierzy:

● 24 szt. dysków 3,8TB SSD-SAS

● 24 szt. dysków 1,8TB SAS 10k

Kontrolery

● Macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami.

● Każdy z kontrolerów macierzy musi posiadać po minimum 64GB pamięci podręcznej Cache.

● W przypadku awarii zasilania dane niezapisane na dyski, przechowywane w pamięci kontrolera muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash.

● Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o minimum 4TiB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności zainstalowanych dysków SSD.

● Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach.

● Macierz musi posiadać funkcjonalność automatycznego balansowania obciążenia kontrolerów macierzy przez przełączanie w trybie online volumenów logicznych pomiędzy nimi w zależności od wygenerowanego na nich ruchu. Musi istnieć możliwość wyłączenia tej funkcjonalności z poziomu interfejsu użytkownika.

● Każdy z kontrolerów RAID powinien posiadać dedykowany interfejs RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy.

● Kontrolery macierzy muszą obsługiwać do 240 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów.

● Oferowana macierz musi mieć wyprowadzone 2 porty dualne FC 16Gbps / iSCSI 10Gbps (obsadzone modułami LC MMF) do dołączenia serwerów bezpośrednio lub do sieci SAN na każdy kontroler RAID oraz 4 porty FC32Gbps (obsadzone modułami LC MMF) do dołączenia serwerów bezpośrednio lub do sieci SAN **na każdy kontroler RAID**

● Macierz musi umożliwiać dołożenie dodatkowych portów do transmisji danych na każdy kontroler RAID:

○ 4x SAS 12 Gbps

○ 4x iSCSI 25 Gbps SFP28

○ 4x FC 32 Gbps

○ 4x iSCSI 10Gbps Base-T

○ 4x iSCSI 10Gbps SFP+

○ 2x InfiniBand 100Gbps

○ 4x NVMe over FC (32Gbit/s)

○ 2x IB iSER (100Gbit/s)

○ 2x NVMe over InfiniBand (100Gbit/s)

○ 2x NVMe over RoCE(100Gbit/s)

● Dołożenie portów jw. nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu a w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych.

Poziomy RAID

● Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID:

○ Raid-0

○ Raid-1

○ Raid-3

○ Raid-10

○ Raid-5

○ Raid-6

○ Raid-DDP

● Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID5 i RAID6 musi być realizowane w sposób sprzętowy przez dedykowany układ w macierzy.

● Macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych.

● Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID, czyli zmianę sposobu zabezpieczenia grupy dyskowej z jednego poziomu RAID na drugi.

Dyski

● Oferowana macierz musi wspierać dyski hot-plug:

○ dyski elektroniczne SSD

○ mechaniczne HDD z interfejsem SAS12Gb/s

○ dyski mechaniczne HDD o prędkości obrotowej 7,2 krpm, 10 krpm,

● Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD w rozmiarach 2,5” i 3,5” zainstalowanych w dowolnym module rozwiązania.

● Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug.

● Macierz musi obsługiwać 120 dysków SAS SSD w całym rozwiązaniu, bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami.

● Macierz musi posiadać oprogramowanie do monitoringu stanu dysków, które pozwala na identyfikowanie potencjalnie zagrożonych awarią dysków oraz z poziomu graficznego interfejsu do zarządzania musi być możliwość sprawdzenia stanu zużycia dysków SSD.

● Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy).

● W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego, wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. CopyBackLess).

● Macierz musi pozwalać na zaszyfrowanie danych na dedykowanych do tego dyskach kluczem AES256-bit zgodnie z wytycznymi Information Technology Laboratory przy National Institute of Standards and Technology (NIST).

● Macierz musi posiadać możliwość skasowania wszystkich danych z dysku FDE celem bezpiecznego ponownego użycia w innym środowisku (Secure Erase).

Opcje programowe

● Macierz musi być wyposażona w system kopii migawkowych umożliwiający wykonanie 128 kopii migawkowych.

● Macierz musi umożliwiać zdefiniowanie min. 2048 woluminów (LUN).

● Macierz musi mieć możliwość tworzenia wolumenów łączonych tzw Contetenated.

● Macierz powinna umożliwiać podłączenie logiczne z serwerami i stacjami poprzez min. 512 ścieżek logicznych FC.

● Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy oraz bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych stacji/serwerów.

● Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie.

● Macierz musi posiadać wsparcie dla systemów operacyjnych:

○ Microsoft Windows Server 2019, 2022

○ SuSE Linux Enterprise Server 15, 12

○ Red Hat Linux Enterprise Server 9, 8, 7

○ Oracle Linux 9, 8, 7

○ Solaris 11

○ Vmware vSphere 7.0, 8.0;

● Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI.

● Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, bez konieczności stosowania zewnętrznych urządzeń konwersji. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy, jako tzw. storage-based data replication. Replikacja danych musi być obsługiwana w połączeniu macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych.

● Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych).

● Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy.

Zarządzanie

● Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej.

● Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym.

● Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (minimum Microsoft Edge, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora.

● Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI.

● Wraz z system musi zostać dostarczone narzędzie do monitoringu macierzy w kontekście:

○ wydajności i opóźnień na wolumenach

○ wydajności I/Ops, MB/s

○ trafności w cache

● Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem autentykacji.

● Macierz musi posiadać oprogramowanie pozwalające na integrację Vmware vCenter – provisioning i monitoring macierzy z widoku vCenter

● Macierz musi posiadać wsparcie dla VMware vSphere Storage APIs Array Integration (VAAI)

Gwarancja i serwis

● Całe rozwiązanie musi być objęte minimum 36 miesięcznym okresem gwarancji z naprawą miejscu instalacji urządzenia i z gwarantowanym czasem wizyty technika do końca następnego dnia roboczego od dnia zgłoszenia awarii do organizacji serwisowej producenta macierzy.

● Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej.

● Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia.

● Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych.

● Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia.

● Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty).

● Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – w formularzu ofertowym należy podać adres internetowy strony producenta macierzy, gdzie można zweryfikować wymagane informacje.

# Serwer bazodanowy 2 szt.

Obudowa

Typu RACK, wysokość 2U;

Szyny umożliwiające wysunięcie serwera z szafy stelażowej wraz z ramieniem porządkującym kable z tyłu obudowy;

Możliwość zainstalowania 16 dysków twardych hot plug 2,5”;

Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych;

Zainstalowane 5 szt. dysków SSD SATA 6G 1,92TB MU. Hot-Plug skonfigurowane w RAID podpięte do sprzętowego kontrolera;

Możliwość zainstalowania dysku M.2 NVMe PCIe4.0 x4;

Zainstalowany wewnętrzny napęd DVD-RW;

Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray.

Możliwość zainstalowania dedykowanego wewnętrznego napędu LTO-8.

Płyta główna

Dwuprocesorowa;

Wyprodukowana i zaprojektowana przez producenta serwera;

Możliwość instalacji procesorów 60-rdzeniowych;

Zainstalowany moduł TPM 2.0;

6 złącz PCI Express generacji 5 w tym:

4 fizyczne złącza o prędkości x16;

2 fizyczne złącza o prędkości x8;

Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;

Opcjonalnie możliwość uzyskania 9 aktywnych interfejsów PCI-e;

32 gniazda pamięci RAM;

Obsługa minimum 8 TB pamięci RAM DDR5;

Wsparcie dla technologii:

Memory Scrubbing;

SDDC;

ECC;

Memory Mirroring;

ADDDC;

Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug.

Procesory

Z uwagi na licencjonowanie silnika bazy danych wymagane jest dostarczenie serwera z jednym procesorem 8-rdzeniowym, taktowanie bazowe 3,9 GHz, architektura x86\_64;

osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base 302 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla oferowanego serwera;

Pamięć RAM

512 GB pamięci RAM;

DDR5 Registered 4800MT/s;

Pamięci obsadzone w sposób gwarantujący najwyższa możliwość wydajność;

Kontrolery LAN

Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:

4x 10Gbit Base-T;

Możliwość uzyskania dwóch interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;

Interfejsy LAN zainstalowane w slotach PCI-e:

4x 10Gbit Base-T

Kontrolery I/O

Kontroler SAS RAID dla dysków wewnętrznych posiadający 2GB pamięci cache, obsługujący poziomy RAID: 0, 1, 10, 5, 50, 6, 60 z podtrzymaniem pamięci cache w przypadku utraty zasilania;

Karta FC – dwie dwuportowe karty FC 32Gb pozwalające podłączyć się złączem LC

Porty

Zintegrowana karta graficzna ze złączem VGA z tyłu i przodu serwera;

1 porty USB 3.0 wewnętrzny;

2 porty USB 3.0 dostępne z tyłu serwera;

2 porty USB 3.0 na panelu przednim;

Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;

Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.

Zasilanie, chłodzenie

Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W;

Redundantne wentylatory hotplug.

Zarządzanie

Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;

informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:

karty rozszerzeń zainstalowane w dowolnym slocie PCI Express;

procesory CPU;

pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;

status karty zarządzającej serwera;

wentylatory;

bateria podtrzymująca ustawienia BIOS płyty głównej;

zasilacze;

system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);

Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:

Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;

Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;

Dostęp poprzez przeglądarkę Web, SSH;

Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;

Zarządzanie alarmami (zdarzenia poprzez SNMP);

Możliwość przejęcia konsoli tekstowej;

Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);

Obsługa serwerów proxy (autentykacja);

Obsługa VLAN;

Możliwość konfiguracji parametru Max. Transmission Unit (MTU);

Wsparcie dla protokołu SSDP;

Obsługa protokołów TLS 1.2, SSL v3;

Obsługa protokołu LDAP;

Integracja z HP SIM;

Synchronizacja czasu poprzez protokół NTP;

Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;

Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);

Wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;

Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.

Wspierane OS

Microsoft Windows Server 2022, 2019;

VMWare vSphere 8.0;

Suse Linux Enterprise Server 15;

Red Hat Enterprise Linux 9, 8;

Microsoft Hyper-V Server 2019.

Gwarancja

5 lat gwarancji producenta serwera w trybie on-site z gwarantowaną wizytą technika serwisu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej;

Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;

Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;

Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;

Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty).

Dokumentacja, inne

Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta;

Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;

Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;

W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;

Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;

Należy dostarczyć i wstępnie skonfigurować system zarządzania infrastrukturą IT. Musi być możliwość monitorowania stanu środowiska IT minimum dla oferowanego serwera oraz biblioteki taśmowej. System zarządzania posiada jeden spójny interfejs GUI HTML do zarządzania całym oferowanym środowiskiem sprzętowym. System zarządzania opiera się o tzw. Virtual Appliance kompatybilny z platformą wirtualną VMware vSphere, Microsoft Hyper-V, KVM. System zarządzania umożliwia aktualizację oprogramowanie systemowego (firmware) na serwerach w zakresie wszystkich istotnych elementów sprzętowych min: BIOS, kontrolery RAID, kontrolery KVM, karty sieciowe. System zarządzania posiada wsparcie dla następujących mechanizmów komunikacji zewnętrznej: HTTPS, SNMP, IPMI. System zarządzania musi mieć możliwość wyeksportowania inwentarza środowiska co najmniej w postaci pliku CSV.

Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 8 - 85 %;

Zgodność z normami: CB, RoHS, WEEE oraz CE.

# Serwer wirtualizacyjny 3 szt.

Obudowa

Typu RACK, wysokość 2U;

Szyny umożliwiające wysunięcie serwera z szafy stelażowej wraz z ramieniem porządkującym kable z tyłu obudowy;

Możliwość zainstalowania 16 dysków twardych hot plug 2,5”;

Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych;

Zainstalowane 3 szt. dysków SAS 12G 600GB 10000 obr./min. Hot-Plug skonfigurowane w RAID podpięte do sprzętowego kontrolera;

Możliwość zainstalowania dysku M.2 NVMe PCIe4.0 x4;

Zainstalowany wewnętrzny napęd DVD-RW;

Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray.

Możliwość zainstalowania dedykowanego wewnętrznego napędu LTO-8.

Płyta główna

Dwuprocesorowa;

Wyprodukowana i zaprojektowana przez producenta serwera;

Możliwość instalacji procesorów 60-rdzeniowych;

Zainstalowany moduł TPM 2.0;

6 złącz PCI Express generacji 5 w tym:

4 fizyczne złącza o prędkości x16;

2 fizyczne złącza o prędkości x8;

Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;

Opcjonalnie możliwość uzyskania 9 aktywnych interfejsów PCI-e;

32 gniazda pamięci RAM;

Obsługa minimum 8 TB pamięci RAM DDR5;

Wsparcie dla technologii:

Memory Scrubbing;

SDDC;

ECC;

Memory Mirroring;

ADDDC;

Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug.

Procesory

Dwa procesory 24-rdzeniowe, taktowanie bazowe 2,9 GHz, architektura x86\_64;

osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base 685 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla oferowanego serwera;

Pamięć RAM

1024 GB pamięci RAM;

DDR5 Registered 4800MT/s;

Pamięci obsadzone w sposób gwarantujący najwyższa możliwość wydajność;

Kontrolery LAN

Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:

4x 10Gbit Base-T;

Możliwość uzyskania dwóch interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;

Interfejsy LAN zainstalowane w slotach PCI-e:

4x 10Gbit Base-T.

Kontrolery I/O

Kontroler SAS RAID dla dysków wewnętrznych posiadający 2GB pamięci cache, obsługujący poziomy RAID: 0,1,10,5,50,6,60 z podtrzymaniem pamięci cache w przypadku utraty zasilania;

Karta FC – dwie dwuportowe karty FC 32Gb pozwalające podłączyć się złączem LC

Porty

Zintegrowana karta graficzna ze złączem VGA z tyłu i przodu serwera;

1 porty USB 3.0 wewnętrzny;

2 porty USB 3.0 dostępne z tyłu serwera;

2 porty USB 3.0 na panelu przednim;

Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;

Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.

Zasilanie, chłodzenie

Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W;

Redundantne wentylatory hotplug.

Zarządzanie

Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;

informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:

karty rozszerzeń zainstalowane w dowolnym slocie PCI Express;

procesory CPU;

pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;

status karty zarządzającej serwera;

wentylatory;

bateria podtrzymująca ustawienia BIOS płyty głównej;

zasilacze;

system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);

Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:

Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;

Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;

Dostęp poprzez przeglądarkę Web, SSH;

Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;

Zarządzanie alarmami (zdarzenia poprzez SNMP);

Możliwość przejęcia konsoli tekstowej;

Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);

Obsługa serwerów proxy (autentykacja);

Obsługa VLAN;

Możliwość konfiguracji parametru Max. Transmission Unit (MTU);

Wsparcie dla protokołu SSDP;

Obsługa protokołów TLS 1.2, SSL v3;

Obsługa protokołu LDAP;

Integracja z HP SIM;

Synchronizacja czasu poprzez protokół NTP;

Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;

Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);

Wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;

Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.

Wspierane OS

Microsoft Windows Server 2022, 2019;

VMWare vSphere 8.0;

Suse Linux Enterprise Server 15;

Red Hat Enterprise Linux 9, 8;

Microsoft Hyper-V Server 2019.

Gwarancja

5 lat gwarancji producenta serwera w trybie on-site z gwarantowaną wizytą technika serwisu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej;

Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;

Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;

Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;

Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty).

Dokumentacja, inne

Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta;

Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;

Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;

W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;

Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;

Należy dostarczyć i wstępnie skonfigurować system zarządzania infrastrukturą IT. Musi być możliwość monitorowania stanu środowiska IT minimum dla oferowanego serwera oraz biblioteki taśmowej. System zarządzania posiada jeden spójny interfejs GUI HTML do zarządzania całym oferowanym środowiskiem sprzętowym. System zarządzania opiera się o tzw. Virtual Appliance kompatybilny z platformą wirtualną VMware vSphere, Microsoft Hyper-V, KVM. System zarządzania umożliwia aktualizację oprogramowanie systemowego (firmware) na serwerach w zakresie wszystkich istotnych elementów sprzętowych min: BIOS, kontrolery RAID, kontrolery KVM, karty sieciowe. System zarządzania posiada wsparcie dla następujących mechanizmów komunikacji zewnętrznej: HTTPS, SNMP, IPMI. System zarządzania musi mieć możliwość wyeksportowania inwentarza środowiska co najmniej w postaci pliku CSV.

Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 8 - 85 %;

Zgodność z normami: CB, RoHS, WEEE oraz CE.

# Rozbudowa switch FC 2 szt.

Rozbudowa posiadanych switchy FC DS-7720b o dodatkowe zalicencjonowane (dostarczyć jeśli jest to wymagane) porty FC w ilości co najmniej 16 szt w konfiguracji 32Gb. W przypadku gdy producent wymaga wznowienia i przedłużenia wsparcia dla urządzeń, należy takowe wsparcie dostarczyć.

# Baza danych 2 szt.

|  |  |  |
| --- | --- | --- |
| **Nazwa silnika bazy danych:** *podaj nazwe* | |  |
| **Wersja:** *podaj wersje* | |  |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **TAK/ NIE** |
| **Oprogramowanie** | Oferowany motor bazy danych musi być dostępny zarówno na platformy systemów operacyjnych Windows i Linux. |  |
| Oferowany Motor bazy danych HIS musi mieć możliwość rozbudowy do wersji wspierającej możliwość synchronicznej replikacji danych w dwóch niezależnych centrach danych. |  |
| Oferowany Motor bazy danych HIS posiada komercyjne wsparcie producenta. Nie dopuszcza się zastosowania RBD typu open-source. |  |
| Oferowany Motor bazy danych HIS ma możliwość realizacji kopii bezpieczeństwa  w trakcie działania (na gorąco). |  |
| Oferowany Motor bazy danych generuje kopie bezpieczeństwa automatycznie  (o określonej porze) i na żądanie operatora oraz umożliwia odtwarzanie bazy danych z kopii archiwalnej, w tym sprzed awarii. |  |
| Oferowany Motor bazy danych umożliwia eksport i import danych z bazy danych  w formacie tekstowym z uwzględnieniem polskiego standardu znaków. |  |
| Administrator posiada możliwość wyboru danych, które mają być monitorowane  w logach systemu z dokładnością do poszczególnych kolumn w tabelach danych, a zarządzanie nimi może odbywać się z poziomu narzędzi do zarządzania bazami danych (dopuszcza się narzędzie na poziomie motoru bazy danych). |  |
| HIS posiada mechanizmy umożliwiające zapis i przeglądanie danych o logowaniu użytkowników do HIS pozwalające na uzyskanie informacji o czasie i miejscach ich pracy. |  |
| Hasła użytkowników są przechowywane w bazie danych w postaci niejawnej (zaszyfrowanej). |  |
| W HIS są zaimplementowane mechanizmy walidacji haseł zgodnie z wymaganiami ustawowymi przewidzianymi dla rodzaju danych przetwarzanych przez HIS. |  |
| HIS umożliwia automatyczne wylogowanie użytkownika z systemu (przy przekroczeniu zadanego czasu bezczynności ustanowionego uprzednio przez Administratora). |  |
| Dostępność oprogramowania na współczesne 64-bitowe platformy Unix (HP-UX dla procesorów PA-RISC i Itanium, Solaris dla procesorów SPARC i Intel/AMD, IBM AIX), Intel/AMD Linux 32-bit i 64-bit, MS Windows 32-bit i 64-bit. Identyczna funkcjonalność serwera bazy danych na ww. platformach |  |
| Niezależność platformy systemowej dla oprogramowania klienckiego / serwera aplikacyjnego od platformy systemowej bazy danych |  |
| Możliwość przeniesienia (migracji) struktur bazy danych i danych pomiędzy ww. platformami bez konieczności rekompilacji aplikacji bądź migracji środowiska aplikacyjnego |  |
| Przetwarzanie z zachowaniem spójności i maksymalnego możliwego stopnia współbieżności. Modyfikowanie wierszy nie może blokować ich odczytu, z kolei odczyt wierszy nie może ich blokować do celów modyfikacji. Jednocześnie spójność odczytu musi gwarantować uzyskanie rezultatów zapytań odzwierciedlających stan danych z chwili jego rozpoczęcia, niezależnie od modyfikacji przeglądanego zbioru danych. |  |
| Możliwość zagnieżdżania transakcji – powinna istnieć możliwość uruchomienia niezależnej transakcji wewnątrz transakcji nadrzędnej. Przykładowo – powinien być możliwy następujący scenariusz: każda próba modyfikacji tabeli X powinna w wiarygodny sposób odłożyć ślad w tabeli dziennika operacji, niezależnie czy zmiana tabeli X została zatwierdzona czy wycofana. |  |
| Wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode). |  |
| Możliwość migracji zestawu znaków bazy danych do Unicode |  |
| Możliwość redefiniowania przez klienta ustawień narodowych – symboli walut, formatu dat, porządku sortowania znaków za pomocą narzędzi graficznych. |  |
| Skalowanie rozwiązań opartych o architekturę trójwarstwową: możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych |  |
| Możliwość otworzenia wielu aktywnych zbiorów rezultatów (zapytań, instrukcji DML) w jednej sesji bazy danych |  |
| Wsparcie protokołu XA |  |
| Wsparcie standardu JDBC 3.0 |  |
| Zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym. |  |
| Motor bazy danych powinien umożliwiać wskazywanie optymalizatorowi SQL preferowanych metod optymalizacji na poziomie konfiguracji parametrów pracy serwera bazy danych oraz dla wybranych zapytań. Powinna istnieć możliwość umieszczania wskazówek dla optymalizatora w wybranych  instrukcjach SQL. |  |
| Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy). |  |
| Wsparcie dla procedur i funkcji składowanych w bazie danych. Język programowania powinien być językiem proceduralnym, blokowym (umożliwiającym deklarowanie zmiennych wewnątrz bloku), oraz wspierającym obsługę wyjątków. W przypadku, gdy wyjątek nie ma zadeklarowanej obsługi wewnątrz bloku, w razie jego wystąpienia wyjątek powinien być automatycznie propagowany do bloku nadrzędnego bądź wywołującej go jednostki programu |  |
| Procedury i funkcje składowane powinny mieć możliwość parametryzowania za pomocą parametrów prostych jak i parametrów o typach złożonych, definiowanych  przez użytkownika. Funkcje powinny mieć możliwość zwracania rezultatów  jako zbioru danych, możliwego do wykorzystania jako źródło danych w instrukcjach SQL (czyli występujących we frazie FROM). Ww. jednostki programowe powinny umożliwiać wywoływanie instrukcji SQL (zapytania, instrukcje DML, DDL), umożliwiać jednoczesne otwarcie wielu tzw. kursorów pobierających paczki danych (wiele wierszy za jednym pobraniem) oraz wspierać mechanizmy transakcyjne (np. zatwierdzanie bądź wycofanie transakcji wewnątrz procedury). |  |
| Możliwość kompilacji procedur składowanych w bazie do postaci kodu binarnego (biblioteki dzielonej) |  |
| Możliwość deklarowania wyzwalaczy (triggerów) na poziomie instrukcji DML (INSERT, UPDATE, DELETE) wykonywanej na tabeli, poziomie każdego wiersza modyfikowanego przez instrukcję DML oraz na poziomie zdarzeń bazy danych (np. próba wykonania instrukcji DDL, start serwera, stop serwera, próba zalogowania użytkownika, wystąpienie specyficznego błędu w serwerze). Ponadto mechanizm wyzwalaczy powinien umożliwiać oprogramowanie obsługi instrukcji DML (INSERT, UPDATE, DELETE) wykonywanych na tzw. niemodyfikowalnych widokach (views). |  |
| W przypadku, gdy w wyzwalaczu na poziomie instrukcji DML wystąpi błąd zgłoszony przez motor bazy danych bądź ustawiony wyjątek w kodzie wyzwalacza, wykonywana instrukcja DML musi być automatycznie wycofana przez serwer bazy danych, zaś stan transakcji po wycofaniu musi odzwierciedlać chwilę przed rozpoczęciem instrukcji w której wystąpił ww. błąd lub wyjątek |  |
| Powinna istnieć możliwość autoryzowania użytkowników bazy danych za pomocą rejestru użytkowników założonego w bazie danych |  |
| Baza danych powinna umożliwiać na wymuszanie złożoności hasła użytkownika, czasu życia hasła, sprawdzanie historii haseł, blokowanie konta przez administratora bądź w przypadku przekroczenia limitu nieudanych logowań. |  |
| Przywileje użytkowników bazy danych powinny być określane za pomocą przywilejów systemowych (np. prawo do podłączenia się do bazy danych - czyli utworzenia sesji, prawo do tworzenia tabel itd.) oraz przywilejów dostępu do obiektów aplikacyjnych (np. odczytu / modyfikacji tabeli, wykonania procedury). Baza danych powinna umożliwiać nadawanie ww. przywilejów za pośrednictwem mechanizmu grup użytkowników / ról bazodanowych. W danej chwili użytkownik może mieć aktywny dowolny podzbiór nadanych ról bazodanowych. |  |
| Możliwość wykonywania i katalogowania kopii bezpieczeństwa bezpośrednio przez serwer bazy danych. Możliwość zautomatyzowanego usuwania zbędnych kopii bezpieczeństwa przy zachowaniu odpowiedniej liczby kopii nadmiarowych - stosownie do założonej polityki nadmiarowości backup'ów. Możliwość integracji z powszechnie stosowanymi systemami backupu (Legato, Veritas, Tivoli, OmniBack, ArcServe itd). Wykonywanie kopii bezpieczeństwa powinno być możliwe w trybie offline oraz w trybie online (hot backup) |  |
| Odtwarzanie powinno umożliwiać odzyskanie stanu danych z chwili wystąpienia awarii bądź cofnąć stan bazy danych do punktu w czasie. W przypadku odtwarzania do stanu z chwili wystąpienia awarii odtwarzaniu może podlegać cała baza danych bądź pojedyncze pliki danych. |  |
| W przypadku, gdy odtwarzaniu podlegają pojedyncze pliki bazy danych, pozostałe pliki baz danych mogą być dostępne dla użytkowników |  |
| Wbudowana obsługa wyrażeń regularnych zgodna ze standardem POSIX  dostępna z poziomu języka SQL jak i procedur/funkcji składowanych w  bazie danych. |  |
| Możliwość budowy klastra na węźle obsługiwanym przez maksymalnie 2 procesory |  |
| Motor bazy danych na poziomie wskazanego numeru wersji wydania musi zapewnić wbudowany, własny mechanizm umożliwiający uruchomienia środowiska w konfiguracji klastrowej wykorzystującej dwa węzły jako podstawę architektury rozwiązania. |  |
| Motor bazy danych musi oferować wbudowane rozwiązanie pozwalające na przechowywanie, analizę i wizualizację danych geolokalizacyjnych. |  |
| Motor bazy danych musi oferować wbudowane rozwiązanie pozwalające na analizę powiązań, relacji między danymi wraz z możliwością wizualizacji tych powiązań i przedstawienia ich wraz z relacjami w postaci graficznej. |  |
| Motor bazy danych musi oferować wbudowane rozwiązanie pozwalające na wykorzystanie zaawansowanych mechanizmów statystycznych, modeli danych, funkcjonalności wartościującej, celem tworzenia analiz, modelowania i predykcji danych przechowywanych w silniku bazy. |  |
| **Licencjonowanie i wsparcie** | Licencja bez ograniczeń z zapewnionym 5-letnim wsparciem. |  |
|  | Licencje motoru bazy danych nie mogą ograniczać ilości użytkowników |  |
|  | Licencja motoru bazy danych nie może posiadać ograniczenia co do wielkości przechowywanych danych oraz nie może powodować dodatkowych opłat w przypadku przyrostu danych |  |

# Wirtualizacja

1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.
2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
3. Pojedynczy fizyczny procesor wymaga przypisania do niego licencji w ilości zgodnej z liczbą fizycznych rdzeni, jednak nie mniejszej niż 16 licencji na rdzenie.
4. Licencja na konsolę do zarządzania środowiskiem wirtualnym musi być zawarta w licencji na oferowany wirtualizator. Ilość licencji na konsolę zarządzającą do rozwiązania determinuje sumaryczna ilość posiadanych licencji na rdzenie fizycznych procesorów.
5. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia 24 TB pamięci operacyjnej RAM.
7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe.
9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 20 portów USB.
10. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 4 GB pamięci graficznej.
11. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
12. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
13. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows 7/8/10/11, Windows Server, Amazon Linux 2, macOS, OS X, Asianux, Ubuntu, CentOS, NeoKylin, Debian, FreeBSD, Oracle Linux, RHEL, SUSE, Photon OS.
14. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
15. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
16. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
17. System musi posiadać funkcjonalność wirtualnego przełącznika sieciowego umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
18. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
19. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).
20. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Wsparcie techniczne musi być świadczone bezpośrednio przez producenta oprogramowania. Licencjonowanie nie może odbywać się w trybie OEM.
21. Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności Microsoft Active Directory, Open LDAP.
22. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
23. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych pomiędzy różnymi systemami pamięci masowych.
24. Rozwiązanie musi zawierać funkcjonalność pozwalającą na ominięcie testów inicjalizacyjnych sprzętu fizycznego w celu szybkiego startu wirtualizatora.
25. Rozwiązanie musi zawierać możliwość zabezpieczania maszyn wirtualnych przez rozwiązania antywirusowe firm trzecich bez konieczności instalacji agenta wewnątrz maszyny wirtualnej.
26. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, pomiędzy serwerami fizycznymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej,
27. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, pomiędzy zasobami dyskowymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej,
28. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, jednocześnie między serwerami fizycznymi oraz zasobami dyskowymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej.
29. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.
30. Rozwiązanie musi zapewniać wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania wszystkich funkcjonalności w tym Hyper-V systemu Windows Server na maszynie wirtualnej.
31. Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.
32. Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn, aby w przypadku awarii lub niedostępności serwera fizycznego maszyny, które na nim pracowały, były bezprzerwowo dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym. Mechanizm ten umożliwia zabezpieczenie maszyn wirtualnych wyposażonych w minimum 2 wirtualne procesory.

# System operacyjny

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego na oferowanym serwerze w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze z uwzględnieniem wirtualizacji

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania  7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
   1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
   2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
   3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
   4. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    2. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:
    1. Login i hasło,
    2. Karty z certyfikatami (smartcard),
    3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,

Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,

Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.

Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.

* 1. Zdalna dystrybucja oprogramowania na stacje robocze.
  2. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
  3. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

Dystrybucję certyfikatów poprzez http

Konsolidację CA dla wielu lasów domeny,

Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,

Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

* 1. Szyfrowanie plików i folderów.
  2. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
  3. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
  4. Serwis udostępniania stron WWW.
  5. Wsparcie dla protokołu IP w wersji 6 (IPv6),
  6. Wsparcie dla algorytmów Suite B (RFC 4869),
  7. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
  8. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:

Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

Obsługi ramek typu jumbo frames dla maszyn wirtualnych.

Obsługi 4-KB sektorów dysków

Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra

Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.

Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

1. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
2. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
3. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
4. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
5. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
6. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

# Okablowanie

Zamawiający wymaga dostarczenia wszelkiego okablowania niezbędnego do zestawienia połączeń logicznych oraz elektrycznych pomiędzy urządzeniami wraz z zapasem 10% na potrzeby zapasu magazynowego.

# Usługa migracji, instalacji oraz konfiguracji

Zamawiający wymaga instalacji oraz konfiguracji rozwiązania zgodnie z wytycznymi producenta systemu HIS, gdyż to na jego potrzeby w głównej mierze budowane jest nowe środowisko. Zamawiający wymaga ponadto uruchomienia replikacji pomiędzy macierzami oraz migracji systemów operacyjnych oraz wszelkich usług biznesowych działających na podstawie systemu HIS, w tym rekonfiguracji integracji HL7. Zamawiający wymaga przeprowadzenia testów poprawności działania systemu HIS w nowym, wspieranym przez producenta środowisku. Jednocześnie Zamawiający wskazuje iż wszelkie koszty związane z procesem weryfikacji przez dostawcę systemu HIS ponosi Wykonawca. W skład zadania migracji wchodzi także przeniesienie systemu bazodanowego Zamawiającego oraz rekonfiguracja usług z niego korzystających.